GenAI against humanity: nefarious applications of generative artificial intelligence and large language models

Abstract

Generative Artificial Intelligence (GenAI) and Large Language Models (LLMs) are marvels of technology; celebrated for their prowess in natural language processing and multimodal content generation, they promise a transformative future. But as with all powerful tools, they come with their shadows. Picture living in a world where deepfakes are indistinguishable from reality, where synthetic identities orchestrate malicious campaigns, and where targeted misinformation or scams are crafted with unparalleled precision. Welcome to the darker side of GenAI applications. This article is not just a journey through the meanders of potential misuse of GenAI and LLMs, but also a call to recognize the urgency of the challenges ahead. As we navigate the seas of misinformation campaigns, malicious content generation, and the eerie creation of sophisticated malware, we'll uncover the societal implications that ripple through the GenAI revolution we are witnessing. From AI-powered botnets on social media platforms to the unnerving potential of AI to generate fabricated identities, or alibis made of synthetic realities, the stakes have never been higher. The lines between the virtual and the real worlds are blurring, and the consequences of potential GenAI's nefarious applications impact us all. This article serves both as a synthesis of rigorous research presented on the risks of GenAI and misuse of LLMs and as a thought-provoking vision of the different types of harmful GenAI applications we might encounter in the near future, and some ways we can prepare for them.